STRATEGY RESEARCH PROJECT

INFORMATION SUPERIORITY AS AN AMERICAN CENTER OF GRAVITY: CONCEPTS FOR CHANGE IN THE 21ST CENTURY

BY

LIEUTENANT COLONEL JEFFREY C. HORNE
United States Army

USAWC CLASS OF 2000

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

Information Superiority as an American Center of Gravity: Concepts for Change in the 21st Century

by

Jeffrey C. Horne
United States Army

COL Ralph D. Ghent
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Jeffrey C. Horne, LTC, USA

TITLE: Information Superiority as an American Center of Gravity: Concepts for Change in the 21st Century

FORMAT: Strategy Research Project

DATE: 10 April 2000 PAGES: 33 CLASSIFICATION: Unclassified

America has made a choice; more than any other nation, the United States is dependent on cyberspace. We have embraced new information technologies, and the trappings of the revolution they have ignited, with unbridled enthusiasm. Our homes, schools, businesses, markets, communication systems, and transportation grids rely on information and telecommunication systems beyond expectations of only a decade ago. Accordingly, the information distribution and processing infrastructures supporting the U.S. elements of national power have become strategic assets worthy of a detailed protection plan to ensure their viability against any intruder.

The U.S. Military's vision for the conduct of future wars, Joint Vision 2010, embraces these views and calls for information superiority as a baseline requirement in achieving battlefield dominance in future wars. This paper focuses on the effects of the information revolution and geostrategic change as they relate to evolving national security paradigms and developing military doctrine. We review the informational threat, examine specific incursions, and develop emotive concepts for the defense of military information networks while also presenting rationale for sharing offensive information operation capabilities with our foes. The discussion concludes with strategic recommendations to continue refinement of our efforts to achieve information superiority well into the millennium.

TABLE OF CONTENTS

INFORMATION SUPERIORITY AS AN AMERICAN CENTER OF GRAVITY: CONCEPTS FOR CHANGE IN THE IN THE 21ST CENTURY

> "We live in an age that is driven by information. The ability to acquire and communicate huge volumes of information in real time is critical to success on multiple levels. The computing power to analyze this information quickly, and control of the systems passing this analysis to multiple worldwide users at near simultaneous rates is changing the face of warfare and how we prepare for war. [1]
>
> Former Secretary of Defense William Perry, 1996

America has made a choice; more than any other nation, we are dependent on cyberspace.[2] Our entire national infrastructure is based on inter-networked grids providing digital exchanges of information to electrical power systems, telecommunication exchanges, transportation systems, and international financial/banking networks. Every aspect of our lives depends on maintaining integrity of the information systems that run these infrastructures. Militarily, the Department of Defense identifies the ability to attain accurate, real-time, information as the key element to enable our battlefield dominance in the future.

Joint Vision 2010, the capstone document for the Department of Defense's preparation for operations in the 21st century, identifies information superiority as the technological engine that fuels operational concepts for the new millennium. Information superiority and technological innovation are expected to transform our previous warfighting tenets into four powerful operational concepts: dominant maneuver, precision engagement, full-dimensional protection, and focused logistics. In short, information superiority is the baseline requirement for our country's ability to achieve full spectrum[3] dominance of the U.S. Military over any competitor. [4]

Carl Von Clausewitz described the term center of gravity as any resource serving as the hub of all power for an organization.[5] The concept has become a critical component of our military doctrine and campaign plans over the past several years. Today, center of gravity is defined as a factor, or resource, that is critical to success – one that, if eliminated, enables an entity to be bent to an oppressor's will. Vulnerability is a complimentary concept to center of gravity. Critical vulnerabilities provide pathways to attacking a center of gravity that may weaken a force if not cripple it altogether. [6]

Given this discussion, it seems clear that information superiority is evolving into a strategic and operational center of gravity for military forces in future warfighting environments. The United States must protect these resources at all costs as we can expect belligerent powers to focus a large part of their efforts to exploiting perceived vulnerabilities. Our systems will be attacked. Prevailing requires vigilance. Acquiring and retaining information superiority and battlefield dominance in the future may be facilitated by developments in four key areas:

(1) Attain a full understanding of the implications of the geostrategic environment, and the changes they invoke in the environments in which we operate. This is the sea in which we swim.

(2) Acknowledge the threat to our operational systems and the strategic information infrastructure that feeds it. We must disseminate this knowledge to the common man, and educate our people and ensure they understand the steps they can take to reduce our vulnerabilities.

(3) Attain significant improvements in the defensive capacity for our military Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) capabilities to ensure the protection of our national assets and minimize the influence of those operating against our national interests. Our national information infrastructure has been examined and a national plan has been developed for its defense, but our operational and tactical systems should be analyzed for critical vulnerabilities.

(4) Overtly develop offensive information operations capabilities to enable appropriate, scalable responses to attacks aimed at nullifying our information superiority. Developing offensive capabilities and sharing the potential effects (vice actual tactics, techniques, and procedures) with potential adversaries provide effective deterrent options for the future. The early days of the Cold War provide good lessons in this area.

GEOSTRATEGIC CHANGE – COMPRESSION, TENSION, AND CONSEQUENCES

> "We are convinced that the challenges of the 21st century will be quantitatively and qualitatively different from those of the Cold War and require fundamental change to our national security institutions, military strategy, and defense posture by 2020.[7]"
>
> Philip A. Odeen, Chairman, National Defense Panel, 1999

Hans Moravec, a distinguished technological futurist, states that the developed world is growing more capable and complex faster than ever before.[8] The increasing velocity of technological change is creating a maelstrom that compels us to the conclusion that something profound is happening, an event of historic proportions.[9] The catalyst for the engine of change extends beyond the end of the Cold War, the advent of electronic chips, the personal computer, and the cellular phone. Rather it lies in the more complex realm of inter-netted cyberlife born of globally integrated computers, distributed databases, world-wide telecommunication inter-connectivity, an explosion of space systems, and the synergy of the Information Revolution.

Although such visionary companies as Federal Express, Microsoft, and 3Com may have seen the opportunity for rapid growth by leveraging these advances into increased market share, some admit that they had no idea of the gravity, depth, and speed of information-based innovations that followed their early implementations.[10] A strategic consequence of this rebirth is a wholly new knowledge-intensive way of conducting our lives. Many of us rely on netted information systems to support our decision-making processes to the point that we are ineffective without our information connections (i.e. Internet, e-mail, CNN).

Understanding the implications of what the information revolution has done for us, and to us, is an incredibly complex process. Advances leading to the demise of the industrial age have changed the very fiber of our workforce and the daily routine we follow. It appears that our schools, government, economy, military, political, and diplomatic environments are changed forever. Information is the currency and telecommunications provides the highway to the market. Clearly these great changes provide opportunity, but they also bring great interdependency, lack of control, and vulnerability. [11]

Militarists and their subject medium, warfare, have often evolved along the path of powerful innovations. History is replete with examples of successful military integration of technology in the form of the catapult, the long bow, the rifled barrel, the repeating rifle, the machine gun, the tank, and radar. Each of these implementations was pioneered largely for military application. Today innovation is more pervasive. The commercial sector is driving the process with the military complex being only one of many consumers. We are not in the driver's seat controlling the pace and direction of innovation. This evokes a need for simultaneous co-evolution of geostrategic awareness, organizational redesign, and revised corporate processes.[12] Accomplishing any one of these activities for an organization as large as the United States government, and its defense department, would be challenging. Doing so simultaneously is incredibly difficult.

Powering this process of evolution is a number of rapidly emerging trends that link information technology, key operational applications, and competitiveness. These commercial concepts are taking root in military doctrine following the development of a plethora of papers, speeches, books, and policies on the subject. This methodical debate resulted in the realization that the ability to attain, manage, and distribute information is a matter of strategic importance.[13] The observations provided below paint a picture of the first-order effects of the information revolution and geostrategic change as we evolve to an information-based force.[14]

- The effects of the end of the Cold War and the resultant new world order are not yet totally understood: vulnerability and risk are not as easily defined as they once were. Governments and transnational actors will increasingly influence world events via non-traditional means such as the proliferation of Weapons of Mass Destruction (WMD), long range precision munitions (ABM, PGM, cruise missiles), and information-based attacks.
- Global tension will increase as the balance between "haves and have-nots" widens in the face of outward economic prosperity. Further destabilization will occur due to war, peacekeeping operations, migration, economic hardship, resource shortages (i.e. food, water, fossil fuels), and expanding environmental concerns. Leading states prosper while failing states fall into despair.
- Awareness and growth of the Internet, and the systems that feed it, cause increasing expectations and infrastructure requirements. Governments will experience pressure to constantly upgrade their systems while simultaneously protecting the infrastructure that supports the networks. This will be incredibly expensive given the exponential proliferation of hardware and software solutions.

- Our world economies, political systems, and military structures are interconnected, and thereby dependent, on automated telecommunication links that feed them. The data and information that empowers these knowledge-based systems fuels the elements of our national power. Sensors, computerization, telecommunications, and information distribution will become the trademark of U.S. military operations. Strengths may become vulnerabilities. The information generated by the Global Information Infrastructure (GII) will be a perishable national asset. We can expect increasing friction resulting from denial of service and outright attacks on these systems.
- The advent of advanced weaponry, long-range precision fires, and soldier/system integration techniques make the warrior more capable and expand his individual area of influence while the battlefield itself becomes incredibly lethal. The end result is a potential decrease in the number of actual soldiers in the close fight, an increase in netted cyber/sensor/robotic systems, and a corresponding need for accelerated cognitive processes of leaders.

These are just a few of the issues facing our leaders. Their cumulative effects put the United States government, and its military establishment, in a difficult position. On one hand, we want to be an open society that encourages modern, moral, democratic, technologically forward thinking and world inter-connectivity. Conversely, unbridled openness threatens elements of national power and security. The environment of compressed decision cycles and real-time information exchange moves so fast that leadership becomes the art of managing the unexpected consequences of very complicated, multi-faceted, decision sets. Risks and miscalculations can become exponential. In short, open economies and global interdependence don't necessarily increase world safety and order; it may actually lead to rapid decompression and unexpected responses.[15]

THE THREAT – ACKNOWLEDGMENT, DISSEMINATION, AND EDUCATION.

> We know the threat is real. Indeed, those who seek to challenge us may now prefer to attack computer-controlled systems – our critical infrastructure – rather than challenge us on the field of battle, where America has an overwhelming preponderance of capability. Where once our opponents relied exclusively on bombs and bullets, hostile powers and terrorists can now turn a laptop computer into a potent weapon capable of doing enormous damage.[16]
>
> President Clinton, 1999

The world is more dangerous today than it was before the break-up of the Soviet Union. Allies and hostile nations may not share our excitement with a U.S.-dominated, uni-polar world. It would seem to follow that our focus on achieving dominance in the relatively new information revolution might create friction. The United Kingdom, Germany, France may be comfortable with a near co-equal, or following, role in this endeavor. However, other countries that are less capable may have had enough of U.S. world dominance. Indications are beginning to surface that indicate extreme cases (i.e. failing states, non-state

actors, and criminal elements) may take unconventional steps to thwart our quest for information superiority.

EMERGENT CHANGES TO THE GLOBAL SECURITY PARADIGM

LTG Patrick Hughes, former Director of the Defense Intelligence Agency (DIA), revealed several intriguing aspects regarding the nature of threats in the coming century.[17] He acknowledged that while traditional global strategic threats had greatly diminished with the break-up of the Soviet Union a new set of conditions present a vastly more intense, complex, diverse, and less predictable world. Three elements of this threat present a new global security paradigm that relate directly to information superiority, vulnerability of information infrastructure, and the resultant potential for information attacks directed against the United States:

(1) **Conditions Threatening U.S. Interests:** There is a significant rise in ideologies inimical to U.S. ideals, concepts, and values. Adversaries may practice access denial to key resources, markets, and systems in conjunction with states or organizations with emerging capabilities (economic, technological, military) to undermine our economic position and negate our conventional warfighting superiority.

(2) **Psychology of Conflict - Why Leaders Engage in Warfare:** competition, grounded in antiquity (history and culture), combined with internal or external leadership pressures create competition over access and control of regional markets and resources. Dissatisfaction with present conditions or the perception of the state of future affairs may ignite conflicts and responses that are foreign to our values, ethics, and traditions. Simply stated, simultaneous, exponential changes in all aspects of an entity's culture create imbalance, a loss of equilibrium, and breed tension. When experienced on a national or global scale, in confluence with historical rivalries, the tension can become hyper-explosive in nature. The potential for a very different kind of conflict is growing.

(3) **Increasing Difficulty in Determining the Interaction Between an Adversary's Capability, Intentions, and Will:** All of these elements are becoming increasingly difficult to determine given the global market, and multiplicity of economic, political, and cultural alliances. State-based systems do not necessarily rule. National Will is increasingly transient, ephemeral, and nearly impossible to determine without covert operations (i.e. human intelligence and offensive information system monitoring). The nature of this transnational threat is complex and exceptionally contrary to bureaucratic systems and traditional thinking. Characteristic threats may include:

(a) Networked decentralized offensive operations that are facilitated by the net with constantly increasing speed, information sharing, visibility, anonymity, and effectiveness. Partners may include non-sovereigns, organized crime, terrorists, state players, ethnic/religious

separatists and anti-authority computer hackers. Techniques employed may include Information Warfare, softwar, and asynchronous warfare.[18]

(b) Advent of Symbiotic Swarming.[19] The focus of this technique is to destabilize and disrupt operations. The strength of the attack is the decentralized nature of the operation. It is characterized by thousands of minor attacks with some major actions (violent, non-violent, and largely non-lethal). Vulnerability is difficult to assess, as adversaries may not have a centralized battle plan. The only link between members is their common opposition of specific U.S. policies, viewpoints, and world domination upon which they are targeting their attack.

(c) Belligerents are organized horizontally vice vertically to avoid stoic processes and delays. Their objective is to make money, push their cause, and inflict unconventional damage[20] on their enemies. This streamlined leadership enables an infinitely faster action/reaction cycle that outpaces bureaucratic U.S. vertical command structure.

Third world nations and failing states may use the techniques just presented to impair our ability to pursue our national interests. Continued intervention in pursuit of democracy and humanitarianism may be perceived as violations of cultural values, economic freedom, and national sovereignty. Realizing that they cannot defeat a technologically superior U.S. force, belligerents are forced to compete unconventionally. The most reasonable and desirable option to resolve conflicts via the infosphere. Evidence indicates that we may be receiving the first reports of such meeting engagements.

FIRST BATTLES

Alan D. Campden, a noted theorist on information warfare, states "no nation is more vulnerable than the United States to electronic attacks."[21] Media stories of computer hackers, crackers, and terrorists abound. Whatever the term, international reports indicate that the battlefield is heating up. The attacks are becoming more sophisticated and the warriors are becoming better trained. This is no longer the realm of a frustrated high school student or a computer nerd in search of a challenge. Today's warriors seem compelled to attack with impunity - stealing information of strategic value from locations thousands of miles away. Tomorrow's warriors and terrorists, whether they be state or non-state players, may be able to do more damage with a keyboard than with a bomb.[22]

Military leaders believe information superiority creates an environment of competitive advantage derived from the ability to exploit superior knowledge of the tactical, operational, or strategic situation. Owning the information environment should enable the opportunity to wage short, sharp, limited conflicts produced by precision engagement of military, economic, and diplomatic tools. Information operations provide the tactics, techniques, and procedures (TTP) to attain this superior position – it enables us to collect, process, and disseminate an uninterrupted flow of information while exploiting and denying an adversary's ability to do the same.[23] We can expect victory in future conflicts to come at the hands of the

country best able to exploit the limits of the information domain while simultaneously shutting down an enemy's information distribution system.

Other countries seem to be arriving at the same conclusion and view our efforts as a threat to their very existence.[24] James Adams visited Russia in 1997 and documented severe paranoia regarding U.S. advantages over the Russian government in the area of information technology. The view appears to be the same throughout the country, "the world is in the midst of a new arms race to achieve information superiority; Russia is losing the race, and the government sees this as a threat to their national security."[25] The perceived technology gap is similar to that of the missile gap of the 1950's.

Internally, Russian organized crime rules amongst a challenged government structure and banking industry mired in a morass of bureaucracy that cannot come to grips with the information age. Externally, Russia's economic competitors beat them to market on all fronts via the Internet. Their goods cannot be sold due to what they view as unfair competition. The common perception is that Russia is at war, both at home and abroad; the battlefield is the information highway-and they are losing on all fronts. But are they?

The reports that follow document attacks directed against U.S. systems by a variety of adversaries around the world. While they are not officially state-sponsored attacks, they are interesting in terms of what is being targeted. The intensity and complexity of the attacks are exceeding our legislative/legal processes and challenging the depth and breadth of our diplomatic and military system. These incursions might come to be known as the first battles of the 21st century information war:

- **Moonlight Maze:** Rogue elements within Russia accomplished their first information warfare attack in an attempt to steal some of the nation's most sensitive weapons guidance information and naval intelligence codes. Deputy Defense Secretary John Hamre told a congressional subcommittee that we are in the middle of a cyberwar.[26] Computer systems, private research and development institutes, and military information systems have been plundered in a systematic, synchronized effort to steal our most coveted weapons, technology, and economic information. The offensive began early in 1999 when a startling new method of computer hacking was detected on American information networks. The adversaries entered dozens of installations and industry sites via overseas Internet sites. Over the next few days dozens of infiltration reports came from military installations, the Pentagon, and Washington D.C. Even top secret intelligence and information security installations such as the Navy's Space and Naval Warfare Systems Command (SPAWAR) were breached.[27] Representative Curt Weldon (R-Pa) stated "We're not certain where they went" but other officials stated that the perpetrators achieved "Root Level" access to all information elements in the system.[28] In the end, it was determined that files were removed from print queues, transmitted across the internet to distributed servers around the world, and then back to San Diego with speed that only delayed the printing by a matter of moments. Eventually the attack was traced via back hacking to Russia. There is no firm evidence that this was a state-sponsored attack, but we must remember that one of the payoffs to this kind

of attack is plausible deniability. A White House statement indicated, "We're no longer dealing in a world of disgruntled teenagers, this is long distance, high tech, espionage. It is impossible to overstate the seriousness of this problem."[29]

- **States, Organized Crime, Terrorists, Rogues, and others:** Libya and Iraq are developing information warfare capabilities of their own. The White House indicates that "we see well-funded terrorist groups developing a wide range of anti-information capabilities". [30] U.S. Information Security personnel indicate that our universities, Department of Defense, Department of Energy, and many national infrastructure systems are under attack. Organized crime could also turn out to be a front for various intelligence communities. [31]

- **China Enters the Fray:** China is intensifying its information warfare programs to conduct both offensive and defensive information warfare. Recent new breeds of Chinese hacker software are being employed in such a way that the intruder can learn, adapt, and manipulate data formations. These programs change modes of operation, proliferation techniques and targets based on external stimulation. Some of these products can also go into "sleep mode" with activation coming via time release, external stimulation, or internal actions within the systems itself (opening of a certain file type). According to James Mulvenon of the Rand Corporation, the target so far has been Taiwan's command systems with the ultimate goal of hacking into U.S. military networks that support deployments to the Asian region.[32]

- **NATO Information Systems (Albania and Kosovo):** In November 1998 hackers penetrated a web server and emplaced a message announcing the intent to attack the site if the U.S. did not cease its hostile activities. Later, during the first days of the air attacks in Kosovo, Yugoslavian hackers attacked the Alliance web sites via a "bombardment strategy" and brought down critical Command and Control (C2) networks. E-mail systems were also attacked frequently using advanced viruses.[33]

- **Rome Labs Incident:** Hackers broke into the U.S. Air Force' s prime research and development facility over 150 times, successfully weaving their way through international phone switches to a computer modem in Manhattan. The two hackers took control of the lab's network and eventually took 33 networks off line for several days. It appears that at least one of the hackers was working for a foreign government and succeeded in removing sensitive Air Tasking Order data. They also successfully gained access to NASA's Goddard Space Flight Center, Wright-Patterson Air Force Base Research and Development facility, and later the U.S. Navy Submarine Research facility. When captured in Argentina the perpetrators stated that they had the capability to read and erase

everything on the network.[34] The Air Tasking Order was available for transmission to any source with the ability to pay the price of admission.

Information superiority is clearly a relative capability whose value is derived from the outcome it enables. It is valued not in and of itself but for what it contributes to enabling offensive and defensive operations on the battlefield – even if the battlefield is a virtual one fought on the plains of the information superhighway. Information operations, a topic to be discussed in detail later, provide a new set of weapons for operating in this environment that enable scalable, non-lethal responses to those threatening our national interests. These responses comprise both offensive and defensive responses to the wide variety of threats posed by the rapidly mutating security paradigms of the 21st century. Clearly we must focus first on getting our own house in order before we stretch out and attempt to mold these situations offensively.

ACHIEVING SIGNIFICANT INPROVEMENTS IN THE DEFENSE OF OUR MILITARY C4ISR SYSTEMS

STRATEGIC LINKS - NATIONAL INFORMATION INFRASTRUCTURE PROTECTION

In 1995 the President directed the Attorney General to review the adequacy of our physical infrastructure protection. The results eventually led to the identification of a major flaw in the defense of our information systems that support our way of life. No significant protective systems were identified in the netted cyber-infrastructure of our national systems including air traffic control, electric power distribution, and public transit. The President initiated the development of a variety of critical infrastructure and information systems in response to the situation with Presidential Decision Directive 63 (PDD-63).

PDD-63 called for the protection of critical cyber-systems such that any manipulation or interruption would be brief, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.[35] The plan of action to provide such capability, the National Plan for Information Systems Protection, identifies a rigorous plan to provide such expansive protection. Specific elements of the proposal are focused on (1) preparation and prevention, (2) detection and response, and (3) building a strong foundation of civil education, personnel development, and legal parameters to enable appropriate responses in the future. Implementation of this program should effectively provide our strategic systems with effective defensive protection by 2005. If we have faith in this program, the next question that needs to be addressed relates to what is being done about protecting the links critical to attaining information superiority at the operational and tactical level.

OPERATIONAL AND TACTICAL SYSTEMS – JOINT VISION 2010

As we have readily shown, compression of time, space, and technological development in conjunction with the blurring of the various elements of national power have confused the boundaries between our civil information systems and those of the military. Several virtual networks covered by the National Information System Protection Plan provide key capabilities to our military systems. Specifically, the Global Information Environment (GIE) is a key component in achieving JV 2010 information superiority. The GIE is a worldwide network of information sources, archives, consumers, and architectures that provide the backbone framework for achieving military information superiority.[36] It provides the capability to reach back to the United States (or other protected sanctuaries) to access a wide variety of computers, sensors, networks, and databases via the National Information Infrastructure (NII) and Defense Information Infrastructure (DII).[37] This is accomplished via integrated access to national, corporate, or military service systems to provide commanders with the battlefield picture necessary to dominate our adversaries. The DII environment supports several key capabilities: It reaches vertically and horizontally into space from home station to the Area of Operations (AO); Crosses the continuum of time from pre-alert phase through deployment, conflict, and redeployment; Spans the military and diplomatic spectrum from tactical military missions to economic or political policies and end states; Includes all levels of organizations from the individual soldier or employee to nation states. [38]

Military leaders are aggressively pursuing C4ISR improvements as the paramount technological capability required to enable our ability to respond rapidly to any conflict. An integrated, near-real time C4ISR network would enable warfighters to dominate any situation and optimize daily operations with accurate, timely, and secure information. JV 2010 envisions capabilities to enhance speed, effectiveness, and decisive action of forward deployed and early-entry forces. These capabilities enable the U.S. military to wrest the initiative from numerically superior enemy forces and set the conditions for victory. The principal components of this capability are:

- A robust multi-sensor information grid providing dominant awareness of the battlespace to our commanders and forces.
- Advanced battle management capabilities that allow employment of our globally deployed forces faster and more flexibly than those of potential adversaries.
- An information operations capability able to penetrate, manipulate, or deny an adversary's battlespace awareness or unimpeded use of his own forces.
- A joint communications grid with adequate capacity, resilience, and network management capabilities to support these capabilities as well as the range of communications requirements throughout the force.
- An information defense system to protect our globally distributed communications and processing network from interference or exploitation by any adversary.

All three military departments are focusing their efforts to achieve JV 2010 Information Superiority. Common concepts include supporting forward-deployed commanders with the following capabilities:

Highly webbed information services; access to all tactical, operational, and strategic information services; weapon systems capable of geographic reach, precision, and speed of response; integrated, multi-tiered sensors that are fully synthesized with databases, shooters, and C4ISR processes. The end result of the integration of the various system capabilities is military information superiority and battlefield dominance: the ability to achieve global range, stealth, flexibility, precision fires, lethality, and global awareness. Space systems (i.e. global positioning, communications, and intelligence distribution) are essential to this process. In short, information systems[39] linked via a global grid to combat systems are expected to provide exponential returns in battlefield dominance.

Clearly, we can now begin to see the gravity of the challenge. The Defense Infrastructure Protection Plan, an extension of the National Information System Protection Plan, provides a good start for the defense of DoD information systems. The problem lies in the fact that it focuses on defending strategic-level systems but fails to address operational and tactical systems necessary for achieving battlefield dominance. This is an essential, incredibly challenging aspect of the problem. Each of the services must ensure availability, confidentiality, integrity, and timeliness of the information being exchanged in a manner that is interoperable with yet to be defined top-level system protection. Additionally, technology-induced compression drives parallel development of organizations, processes, doctrine, advanced technology, and technical solutions. Dealing with this chaotic environment of change requires an adaptive form of change management and an engineering mentality.

PROPOSING INTERIM SOLUTIONS

It has taken four years to define a potential solution to protecting our strategic level systems in the form of the National Information Infrastructure Protection Plan (NIIPP). Implementation is expected to take an additional three to five years; all of this in an environment replete with presidential interest, national reviews, and executive directives. How long will it take the Services to respond in kind in a joint manner that assures the defense of JV 2010 information superiority capabilities? While we can anticipate large-scale transference of concepts and processes from NIIPP, we will still require a mandate from the top of our profession to force the issue. This should be a matter of the greatest urgency.

This process requires integration of security enhancements to the vast array of existing legacy systems as well as those yet to be fielded. Services including networked intrusion detection, attack notification, event mitigation measures, and counter-response require a vast array of expensive, technically challenging software/hardware modifications. This task must be accomplished across the joint spectrum from national strategic intelligence/information/telecommunication systems interfaces to operational/tactical military decision support systems.

There is no silver bullet for protecting all systems, nor do I believe all systems require such attention. Many of our information systems are important for the various tasks associated with running any large organization but their loss would not provide catastrophic results on an information intensive battlefield. However, others are essential to maintaining battlefield frameworks of key information sets.

While I am sure the Services are accomplishing some form of review of this situation I believe it is time to consolidate the effort similar to that of the NIIPP but with a more streamlined approach similar to that in which we attacked the perceived Y2K problem. The actions described below provide a baseline on which we could accomplish the task by assessing the situation, educate our people on how they can contribute to enhanced protection against information network attacks, and prioritize the limited resources available to address the situation:

- **Threat Analysis and Dissemination**: The Services must have a common view of the migratory nature of the threat and then ensure a common level of understanding at all levels of the organization. We must get away from various conflicting assessments and disseminate a common understanding to the force. Educated leaders, acquisition teams, system managers, and users could provide innovative procedural and systemic solutions to combat known system shortfalls. Remaining challenges can be incorporated into hardware/software solutions as required.
- **Identify the tactical/operational systems that provide JV2010 information superiority**. This process must identify Joint and Service specific systems providing critical, interoperability information and system flow/support relationships. Mapping the systems permits identification of vulnerable interface points and may also facilitate identification of redundancies suitable for joint applications.
- **Triage the system map** of information generation, storage, and distribution systems against the aspects of what systems contribute the most to full-spectrum battlefield dominance and the tenets of information superiority. Criteria such as criticality, vulnerability, and recouperability could be used to provide quantitative measures to this process. This must be accomplished for both legacy and new systems. Special emphasis should be placed on minimizing redundancies of legacy systems as they pose the greatest challenges for retrofitting defensive solutions. The end result of this process should be a rank ordered set of priorities for resourcing.
- **Identify a DoD executive agent** responsible for integrating resource decisions across Service boundaries. Determining the appropriate organization for this structure is outside the purview of this paper. However, logical candidates for the responsibility could be organized under the auspices of the Assistant Secretary of Defense for Command, Control, and Communications (ASD-C3I) and Chairman of the Joint Chiefs of Staff, The Joint Staff, Washington D.C. The primary responsibility of the office would be to establish an effective relationship with the leaders of the NIIPP[40] and decision authority for available information system defensive protection resources. This office should be responsible for developing short-term technical solutions for information system protection as well as long-term solutions across the domains of Doctrine, Organization, Individual Training and Manning, Logistics, and Leader Development.

- **Establish a plan of action and timeline for corrective actions** that coincides with our effort to defend our national systems. While the threat is perceived to be both real and imminent, an endless study without timelined decision sets would be of little value. As mentioned previously, the interconnected nature of all of our systems is growing to the point that we are only as strong as our weakest link. However, we must draw a line in the sand, set a deadline as we did with the Y2K process, and treat it with the same level of reverence.

OVERT DEVELOPMENT OF OFFENSIVE INFORMATION OPERATION CAPABILITIES

> Information warfare is a broad national security problem. It is not unique to a particular environment, specific type of warfare, or force. It is something that affects every American and consequently deserves the same level of attention. We did not create a separate warfare area for nuclear warfare but we did create an environment where the various disciplines could come together and be managed together in similar work and career paths. Fundamental things have to change, the pace has to increase, and wargaming/modelling has to happen quickly. [41]
>
> Vice Admiral Cebrowski, former Joint Staff J-6.

We have discussed the effects of geostrategic change, evolving security challenges, and defensive measures necessary to combat the associated threats as they relate to the development of information superiority. The next step in assuring battlefield dominance via information superiority is the development of an effective counter punch that enables the force to go on the offensive and defeat the enemy on our own terms. Clearly we are developing conventional forces to accomplish this task, but the ideal situation is being able to win without ever having to place a warship in harms way or forcing a soldier to set foot on foreign soil. Offensive information operations provide the opportunity to conduct such a battle. At the very least offensive IO provide tools that are critical to gaining battlefield dominance in the 21st century.

POLICY, DOCTRINE, RESPONSIBILITIES

While we have talked in great detail regarding the basis for information superiority requirements and the challenges we face in that regard, we have only tacitly referred to information operations and its role in achieving battlefield dominance. A concise review of the concept of IO followed by its role as an offensive tool is in order prior to discussing the ramifications of overtly developing offensive capabilities. Previously I referred to IO as a set of tactics, techniques, and procedures (TTP) that were both offensive and defensive in nature that enable information superiority and quantum contributions to battlefield dominance. Doctrine articulates IO as "actions taken to affect adversary information (and information systems) while defending one's own systems (information, systems, processes, and networks).[42]

The Department of Defense and the Joint Staff published the first definitive guidance on Information Operations in November and December 1998. These documents, reflecting years of

intellectual discussion and research, identify specific responsibilities and layout concepts for managing this complex environment. The policy addresses a variety of strategic issues, realms of operation, and specific responsibility. The doctrinal publication, JCS Pub 3-13, compliments the policy with thorough procedural details for implementation. The joint policy focuses on identifying strategic vulnerabilities and discusses offensive and defensive efforts directed against specific targets: decision makers and the infrastructure that supports them (the information itself, communications transfer links, information gathering and processing nodes, and human interfaces).[43]

Offensive information operations are described as those that influence, deny, degrade, disrupt, destroy, deceive, the target in a manner that is mutually supportive to other policies and objectives.[44] Strategically, U.S. information operations are being developed to provide effective deterrence to diffuse crises and reduce confrontation. The end goal will hopefully maximize the effectiveness of the national elements of power to an extent that military operations are used only as a last resort. It is widely believed that the release of this doctrine has taken a large step to institutionalize the process from its ad hoc origins and identifies IO as a global issue.[45]

Recent changes to the Unified Command Plan (UCP) assigned responsibility for offensive and defensive information operations to U.S. SPACECOM. This action takes the first steps in operationalizing the concepts of information operations into traditional force structures of the U.S. Military. Joint Task Force Computer Network Defense (JTF-CND)[46] enables U.S. SPACECOM to provide unified, global operational focus for the military's computer network defense mission and capitalizes on the links between space and information operations. JTF-CND coordinates with the National Infrastructure Protection Center (NIPC) to coordinate its services with other federal agencies. The UCP expands U.S. SPACECOM's charter to include Computer Network Attack (CNA) in October 2000.

One of the first issues facing the Command in their new role will be one of clarifying roles, missions, and expectations in the arena of Information Operations. While the strategic issues facing network defense may be relatively clear at this point, those of offensive operations and network attack are not. The ability to maintain information superiority for the force depends on our ability to successfully navigate this difficult path. Specifically, our ability to respond appropriately, and offensively, to asymmetric attacks directed against our infrastructure will become a matter of incredible strategic importance. We can expect that our response will either diffuse the situation or promote escalation. We should also understand that in the views of many nations, strength of response is also a show of resolve. This has particularly important ramifications regarding emerging global security paradigms discussed earlier.

AVOIDING A COLD WAR MENTALITY

A review of our policies on offensive information operations reveals an approach similar to that of nuclear development in the early years of the Cold War. There is little or no discussion of our capabilities in unclassified forums and any mention of the use of offensive tools evokes hushed discussions and movement to protected conference rooms. Procedures for controlling the use of offensive capabilities are

managed at the highest levels of the chain of command. Information Operations Conditions (INFOCONs) are being developed similar to Threat Conditions (THREATCONS) and Defense Conditions (DEFCONs) of years gone by. All are established for noble causes and are necessary to heighten awareness, mitigate damage, and authorize varying responses to belligerent acts. INFOCONs accomplish these tasks but also assess if initial assaults are part of larger scale campaigns directed against our country that mandate actions to mitigate the situation.[47] The challenge is not one of procedures as much as perception; discussions of INFOCONs elicit flashbacks to nuclear special access programs, clandestine activities, secrecy, and fear.

A review of what we learned about the effects of clandestine secrecy and legal issues during the nuclear arms race provide valuable insights as we negotiate our path into the arena of offensive information operations. This abbreviated analysis does not provide the answers to all questions on the subject. The goal of this discussion is a simple one; the hope of evoking thought and creative viewpoints worthy of consideration and potential employment.

The nuclear arms race and the Cold War traveled hand in hand from 1947 to 1989. George Kennan stated that the basis for the effort was patient, long-term, containment of the Russian expansionist tendencies following WWII. The execution of the policy became what Winston Churchill termed as the Cold War – a process of Russian clandestine warfare aimed at creating national liberation of oppressed democratic countries. The United States had no activity designed to combat such a war other than the creation of a vast counter-clandestine force under the Central Intelligence Agency (CIA).[48] Throughout the period that followed, the United States and the Soviet Union carved their respective influence into a world order dominated by the threat, and containment, of nuclear war.

The effects of inter-secrecy between countries, and the intra-secrecy within the nation, sometimes exaggerated the threat and terrorized the people, but it also served as a galvanizing influence overall. However, in the end, unchecked clandestine activities and unquestioned governmental threat assessments came to an end with congressional reviews and subsequent oversight in 1975-76.[49] This marked an end to extraordinary authority for conducting secret operations and began an era of openness of American society. Congressional oversight and media involvement took on new dimensions. In 1980 we saw the election of a new president and the beginning of an unprecedented military peacetime buildup. President Reagan's unprecedented build-up of conventional military forces combined with openly parlaying the capabilities of our nuclear programs, followed by our commitment to the Strategic Defense Initiative (SDI) appear to be the straws that broke Soviet resolve and brought about the downfall of the USSR.

Winning the long showdown with the Soviets was an amazing governmental achievement. We managed to convince a nation wary of large militaries and governmental regulation to spend 13 trillion dollars on defense while somehow retaining a burgeoning economy.[50] Historians focus on the succession of wars in the budget process, on the battlefields of Korea, the Bay of Pigs, and Vietnam. I tend to agree with those that saw us win the transition from mass-produced, mass-equipped armies of

WWII to a high technology force that devastated Russian-trained and equipped Iraqi soldiers and won Desert Storm. A coin of the realm in this process was ending the secrecy and showing the world our capabilities and our resolve. Moscow finally understood that they could not compete with a high technology force backed by a seemingly endless fiscal commitment.

DEVELOPMENT OF INTERNATIONAL PRINCIPLES

Clearly, today's world differs greatly from that of the Cold War, but the lesson of openness remains. Although we have a unipolar world in 2000, we have no idea how the world order will evolve in the very near future. Multiple countries have nuclear, conventional, and now informational capabilities that create a complex national security web. Information can be checked via hundreds of sources, imagery is available on the Internet, secrets are incredibly hard to keep. Our best course is to do everything in our power to convince the American people, and the world, that we can defend our country with a range of capabilities and our desire is a simple one – that of protecting our national interests. We will do so in such a way as to maximize fairness and equitability while maintaining the sovereignty and human rights around the world. We wish to do so in a way that is swift, unobtrusive, economical, and protects the lives of innocent people. Offensive information operations are a critical tool in this process.

A policy of openness on the issue of offensive information operations does not mean that we expose our sources, tactics, techniques, or procedures. However, it is critical that we ensure that the world understands our resolve and the capability for unconventional precision targeting of both kinetic weaponry and cyber-attacks. Critical to this strategy is the conduct of a public information campaign that presents our capabilities to both adversaries and allies. Although an information arms race is possible, we may find that information sharing, technical exchange, and firm diplomatic/economic/military resolve will mitigate this problem. A set of international principles would facilitate this process. Recommendations along these lines include:

- Maintain the right to explore offensive and defensive operations in the interests of national security.
- Engage in information sharing with those that are interested. However, there is no virtue in the development of unilateral treaties and negotiations. We will entertain the development of United Nations rules of behavior for nation states and registered non-state players and cross-linking of large-scale alliances such as NATO and OPEC.
- Affirm that information, and the systems over which it is transported, is state property and should be afforded all the rights of national sovereignty when operating in international space. Interfering, disrupting, destroying, or falsifying data within these confines is accords appropriate unilateral or international sanctions.
- Assert the right to unimpeded virtual travel and operation across international information/telecommunication systems as long as one operates within accepted international principles.

- Acknowledge offensive information operations as a scalable means to avert lethal conflict and air/ground/sea force deployments. The United States can employ offensive IO to establish global presence from distant locations. Agreements between the international community designed to permit denial of services to those violating ascribed principles could go a long way to prevent regional adventurism.

NATIONAL IMPLICATIONS - CONCLUSIONS AND RECOMMENDATIONS

> In preparations for national defense we have to follow an entirely new course because the character of future wars is going to be entirely different from that of past battles... We had better get accustomed to this idea and prepare ourselves for the new conflicts to come.[51]
>
> Giulio Douhet

National leaders have long recognized the paramount importance of decisions for war or peace. These decisions must be taken with utmost deliberation. Careful evaluation of a specific situation against rigorous criteria should always precede each decision to employ US military force (e.g., combat force in a hostile environment). As a minimum, these criteria must establish for the strategic decision-maker an assessment of acceptability (political support of our leadership and eventually our populace), feasibility (appropriate levels of forces and resources), and suitability (well-defined objectives matched by an effective plan).

We must weigh these criteria heavily before entering into any conflict but we must also recognize that a new arrow has been placed in our national military quiver. As with mechanized warfare, strategic bombing, and air superiority, it sometimes takes a while for military thinking to catch up with technology. But bear no mistake that information superiority and information operations have emerged as the next area of operational battlespace requiring our attention. This is especially true in the area of offensive operations. LTG (R) Douglas Buckholtz, former Director for Command, Control, Communications, and Computers (J-6), Joint Staff states, "Our challenge, is to get Kinetic Warriors – colleagues who see tanks, planes, and ships as the main tools of war – to understand and accept that networks and full-scale Information Operations are better than traditional weapons in many situations." [52]

So, where does this leave us? The United States has achieved world prominence in the arenas of politics, economics, diplomacy, and military strength. Our allies often place us in the position of serving as the world's conscience with the second order effect of making the American military the first choice of many nations requiring force to solve their problems. Additionally, our senior leaders have articulated a vision that mandates dominance across the spectrum of conflict. Information superiority is the lynchpin in achieving this position as we proceed into the new millennium. Most would agree that this is an aggressive strategy.

Prudence dictates that we take a step back and determine what actions must be taken to protect our tactical and operational information systems to ensure our ability to maintain uninterrupted information flow to field commanders. We should attack this challenge with the same level of effort as we did with the Y2K challenge. Using the national infrastructure protection plan as a baseline model may provide a strategy to attack this problem. The bottom line is we must be able to respond to the inevitable attacks to come. Reviewing and possibly adjusting our azimuth toward reliance on information superiority may be the best path. In the words of Theodore Roosevelt, "nine-tenths of wisdom is being wise just in time." [53] The recommendations that follow are intended to provide a menu of strategic concepts necessary for our civilian and military decision-makers as we develop our National Security and National Military Strategies for the new millennium.

(1) **Continue to focus on the Threat After Next via Futures Related Exercises:** It appears that there is no single document or concept that depicts a view of the threat facing military forces in the next few years. Although the general concepts seem to permeate many documents, a common operational or strategic picture of the battlefield fails to exist. This situation is especially evident in the area of asymmetric threats directed against the United States. It would be helpful if the President directed the development of a threat analysis applicable to all elements of national power to develop synergy across agencies and departments.

(2) **Continue to push the development of defensive capabilities with great haste**. We must determine our vulnerabilities once we have a common understanding of the threat, and it is disseminated to both our military and civil populace. We can then triage the key systems involved and identify tactical and operational system improvements. Accomplishing this effort mandates a single Service and DOD official(s) responsible to the JCS for developing systemic solutions across the joint spectrum.

(3) **Overtly develop an offensive capability** with the well-publicized intent of avoiding military – boots on the ground/precision weapon engagements. An objective of this effort would be to minimize the constantly increasing number of US military forces being deployed around the globe. Offensive information operations provide the opportunity to reduce, not eliminate these deployments. This capability also provides our national leaders with a scalable electronic attack capability that may destroy a belligerent's capability, prestige, and support (resources and political/popular backing), without endangering innocent lives.

(4) **Develop a selective engagement doctrine** – The Weinberger Doctrine has long been discarded as too restrictive in today's environment. However, information operations provide a spectrum of tools capable of selectively engaging belligerents around the world. Its capability to conduct precision engagement, either lethal or non-lethal, is a valuable tool to be considered for developing selective engagement policies of the future. Information Operations provide interesting alternatives in ascending the ladder of aggression between political sanctions, flexible Deterrent Options (FDO), and lethal actions to deter crisis.

(5) **Promote the Value of Futures Thinking and Exercises:** There is great value in institutionalizing future thinking in organizations, exercises, and combat developments. While it is true that there are no facts about the future, only predictions, it makes sense to work through the issues even if the endstate prediction is wrong. The value comes in critical thought that comes throughout the process. History seems to indicate that in times of rapid change organizations that keep pulse survive. Failure to institutionalize/internalize change causes them to perish.

WORDCOUNT = 8413

ENDNOTES

[1] Robert Whisenhunt. Information Warfare and the Lack of a U.S. National Policy, Strategy Research Project. Carlisle Barracks: U.S. Army War College, 18 July 1996, 2.

[2] William Clinton. National Plan for Information Systems Protection, Washington D.C.:The White House, Jan 2000, 21.

[3] Department of the Army, Operations, Field Manual 100-5 (Draft). (Washington D.C.: U.S. Department of the Army. Jan 00), 18. Full spectrum dominance is defined as the ability to win a full range of conflict situations ranging from disaster relief and humanitarian assistance to a Major Regional Conflict (MRC).

[4] Joint Chiefs of Staff. Concept for Future Joint Operations: Expanding JV 2010, Washington D.C.: The Joint Staff, May 97.

[5] Peter Paret. Makers of Modern Strategy-From Machiavelli to the Nuclear Age, Princeton. Princeton University Press, 213.

[6] U.S. Department of the Navy, United States Marine Corps, Warfighting ,MCDP 1, (Washington D.C.: U.S. Department of the Navy, Headquarters United States Marine Corps, 20 June 1997, 46-47.

[7] Philip Odeen. Transforming Defense, National Security in the 21st Century, Arlington: National Defense Panel, December 1997, 3.

[8] Hans Moravec. Robot: Mere Machine to Transcendent Mind. New York: Oxford University Press, 1999, 1.

[9] The ideas in this paragraph are based on remarks made by a speaker participating in the AWC Commandant's Lecture Series.

[10] Larry Downes, and Chunka Mui. Killer App: Digital Strategies for the Market Place, Boston: Harvard Business School Press, 1998, 13.

[11] Michael J. Stewart. Information Operations, Information Warfare: Policy Perspectives and Implications for the Force, Strategy Research Project. Carlisle Barracks: U.S. Army War College, 24 July 1997, 5.

[12] David Alberts, John Garstka, and Frederick P. Stein. Network Centric Warfare, Developing and Leveraging Information Superiority. DoD C4ISR Cooperative Program. Washington D.C., 1999, 13.

[13] Stephen Klinefelter. National Security Strategy and Information Warfare, Strategy Research Project. Carlisle Barracks: U.S. Army War College, 23 July 1997. 2-4.

[14] Vast arrays of studies have come to similar conclusions about the array of issues we will face in future years. These extensive lists were coalesced to the relatively short depiction provided in this paper. A more detailed presentation can be found in the conclusions of the U.S. Joint Strategy Review, the National Defense Panel, and the after action reports of the Services futures-related wargames. (i.e. Army After Next).

[15] Alvin Toffler, and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. New York: Little, Brown, 1993, p 212.

[16] William Clinton. National Plan for Information Systems Protection. Washington D.C.:The White House, January 2000, vi.

[17] Congress, Senate, Select Committee on Intelligence, Global Threats and Challenges: The Decades Ahead, Statement of LTG Patrick Hughes, 28 January 1998, 4.

[18] Ibid, 7. These forms of waging war provide the greatest flexibility to an adversary, span the entire range of conflict, thus making them the most likely to be encountered at all levels. All involve information systems either directly or indirectly. The most common and potent elements include; (1) Information Warfare - actions taken to degrade or manipulate and adversary's information system while defending your own. (2) Softwar - Information Warfare designed to disrupt, deny, corrupt, or destroy information resident in computers, local or wide area networks, and global information systems (3) Transnational Infrastructure Warfare – attacking key industries, utilities and systems supporting a nation's national power base. (I.e. telecommunications, energy, power, transportation, banking, government operations, air traffic control, emergency services, distributed manufacturing networks.) (4) Asymmetric Warfare – Attacking an enemies weaknesses while preventing him from doing the same to you. Ultimately the objective is to attack the enemy with a capability that they have no capability to respond to. (5) Asynchronous Warfare - Preselected or delayed attacks on an adversary taking advantage of the passage of time to develop a strategic opportunity to exploit future vulnerabilities, 7.

[19] Stephen Metz, Ph.D. Draft Paper: Military Strategy and information Technology: Alternative Visions of Future War. Carlisle Barracks: Strategic Studies Institute, U.S. Army War College, 1999, 16.

[20] Ibid, 18. They will attempt to avoid direct conventional attacks with weaponry. They are outmatched by U.S. forces that could be used against them in retaliatory attacks. Their focus is to steal information and use it against us, debilitate our information networks, disrupt our infrastructure (i.e. transportation, markets, support systems) to weaken our national will.

[21] Whisenhunt, 5.

[22] Toffler, 151-152.

[23] David Alberts, John Garstka, and Frederick Stein. Network Centric Warfare, Developing and Leveraging Information Superiority. DoD C4ISR Cooperative Program, Washington D.C.: 1999, 54.

[24] James Adams. The Next World War, New York: Simon and Schuster, 1998, 233-238.

[25] Ibid, 265.

[26] Gregory Vistica. "We're in the Middle of a Cyberwar," Newsweek, 20 September 1999, 89.

[27] Ibid, 91.

[28] Matthew Campbell. "Russian Hackers Steal U.S. Weapons Secrets." London Sunday Times, July 25, 1999, 19.

[29] Ibid, 20.

[30] Vistica, 91.

[31] Ibid, 92.

[32] Vernon Ehlers. "Information Warfare and International Security," THE OFFICER. Vol. 75, Sep 1999, 30.

[33] Ibid, 33.

[34] David DiCenso. "IW Cyberlaw: The Legal Issues of Information Warfare." Airpower Journal, Summer 1999. From Jack L. Brock's, Testimony before GAO Committee on Government Affairs, U.S. Senate Permanent Subcommittee on Investigations, "Information Security: Computer Network Attacks at Department of Defense Pose Increasing Risks", GAO/TAIMD-96-2, 18.

[35] William Clinton. National Plan for Information Systems Protection. Washington D.C.:The White House, January 2000, viii. PDD-63 defined critical infrastructure cyber-systems as those that are so vital to the Nation that their incapacitation or destruction would have a debilitating impact on national economic, military, or political security and/or national public health and safety.

[36] Chairman Joint Chiefs of Staff. Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance, The Joint Staff, 4 July 1995, 36.

[37] Ibid, 36. The NII and DII components are a network of networks comprising intelligence, C4I, databases, electronics, personnel systems supporting the commander at tactical, operational and strategic levels.

[38] Department of the Army. Information Operations, Army Field Manual 100-6. Washington D.C.: U.S. Department of the Army, 30 August 1996, 1-4.

[39] Louis Caldera and Dennis Reimer. A Statement on the Posture of the U.S. Army Fiscal Year 2000, Washington D.C.: U.S. Department of the Army, February 1999, 44. Specific Army combat developments supporting the world-wide information grid include the Army Tactical Command and Control System (ATCCS); Force XXI Battle Command Brigade and Below (FBCB2), Maneuver Control Systems (MCS), Air and Ground-Based Sensors, Unmanned Aerial Vehicles, The All Source Analysis System (ASAS), Enhanced Position Location Reporting Systems (EPLRS).

[40] William J. Clinton. National Plan for Information Systems Protection, Washington D.C.:The White House, Jan 2000, 21. Key leaders and their parent organizations in this effort would be the National Coordinator for Security, Critical Infrastructure and counter-Terrorism (NSC), Critical Infrastructure Assurance Office (Commerce Dept), National Infrastructure Protection Center (FBI), and lead agents from each of the Services.

[41] Jason Sherman. "INFOWAR: What Kind of Defense, Armed Forces Journal, August 1997, 28.

[42] Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington D.C.: The Joint Staff, 9 October 1998, GL-7, and 9.

[43] Joint Chiefs of Staff, Joint Information Operations Policy. JCSI 3210.01A, Washington D.C.: The Joint Staff, 6 November 1998, 8-9.

[44] Department of the Army. Information Operations, Army Field Manual 100-6. Washington D.C.: U.S. Department of the Army, 30 August 1996, 16.

[45] Interview at the Navy Connecting Technology Conference with Daniel Kuehl, Chairman of the Information Operations Department, School of Information Warfare and Strategy, National Defense University, Federal Computer Week, Dec 98, 1.

[46] SPACECOM News Release, Directorate of Public Affairs, 1 Oct 1999, 1. JTF-CND was activated on December 30, 1998, after exercises and real-world events demonstrated the need for a single coordinating agency with the authority to direct actions for protecting national computer networks. This 90-100 person organization is collocated with the Defense Information Systems Agency's (DISA) Global Network Operations and Security Center in Arlington, Virginia. Originally, it was understood that this was an interim solution designed to be associated with a unified command of the U.S. military.

[47] The Joint Staff. CJCSI 3210.01A, A-7. THREATCONS are currently discussed only as a part of defensive doctrine. They assist in determining if there is a larger IO campaign (i.e. propaganda, diplomatic attacks, terrorism, deception) directed against the U.S. to achieve adversarial objectives. They also provide an assessment as to what other actions should be taken to protect forces or operations.

[48] Arthur M Cox. The Dynamics of Détente. New York: Norton, 1976, 203.

[49] Harvey M. Sapolsky, Eugene Gholz, and Allen Kaufman. " Security Lessons from the Cold War." Foreign Affairs, July/Aug 1999, 203.

[50] Ibid, 207.

[51] Kevin Kennedy, Bruce Lawlor, and Arne Nelson. Grand Strategy For Information Age National Security. Policy Analysis Paper. Cambridge: Harvard University, John F. Kennedy School of Government, National Security Program, 22 Aug 1996, 101.

[52] Sherman, 28.

[53] Peggy Anderson. Great Quotes from Great Leaders. Lombard, Illinois, Successories Publishing, 1990, 8.

BIBLIOGRAPHY

Adams, James. The Next World War. New York: Simon and Schuster, 1998.

Alberts, David, John Garstka, and Frederick Stein. Washington: Network Centric Warfare, Developing and Leveraging Information Superiority, DoD C4ISR Cooperative Program (CCRP), 1999.

Allard, Kenneth, Command, Control, and the Common Defense. Washington: Center for Advanced Concepts, Technologies, and Information Strategies, National Defense University, October 1996.

Anderson, Peggy. Great Quotes from Great Leaders. Lombard, Illinois, Successories Publishing, 1990.

Bass, Carla. "Building Castles on Sand: Underestimating the tide of Information Operations." Airpower Journal, Vol 15, Summer, 1999, 27-45.

Biddle, Stephen. "Assessing Theories of Future Warfare." Security Studies, Vol 8, Number 1, Autumn 1998, 8-18.

Brewin, Bob. "DoD Recognizes Information Warfare as Key Battlefield System." Federal Computer Week, 2 December 1998, 8-13.

Bushnell, Dennis. Chief Scientist at NASA Research Center, interview by author on the subject of future warfare, 2 June 1999, Langley, Virginia.

Caldera, Louis, and Dennis Reimer. A Statement on the Posture of the U.S. Army Fiscal Year 2000, Washington D.C.: U.S. Department of the Army, February 1999.

Campbell, Matthew. "Russian Hackers Steal U.S. Weapons Secrets." London Sunday Times, 25 July 1999, 19-20.

Clinton, William. A National Security Strategy for A New Century. Washington, D.C.: The White House, October 1998.

____. National Security Science and Technology Strategy. Washington, D.C.: The White House, October 1998.

____. National Plan for Information Systems Protection. Washington D.C.:The White House, January 2000.

Cohen, William. Report of the Quadrennial Defense Review. Washington D.C., The Pentagon, May 1997.

Cox, Arthur. The Dynamics of Détente. New York: Norton, 1976.

DiCenso, David. "IW Cyberlaw: The Legal Issues of Information Warfare." Airpower Journal, Vol 15, Summer 1999. From Jack L. Brock's, Testimony before GAO Committee on Government Affairs, U.S. Senate Permanent Subcommittee on Investigations, "Information Security: Computer Network Attacks at Department of Defense Pose Increasing Risks," GAO/TAIMD-96-2.

Downes, Larry, and Chunka Mui. Killer App: Digital Strategies for the Market Place, Boston: Harvard Business School Press, 1998.

Ehlers, Vernon. "Information Warfare and International Security." THE OFFICER, 75, September 1999, 28-32.

Guthrie, Samuel. Knowledge-based Operations: The "So-What" of Information Warfare. School of Advanced Military Studies, The United States Army Command and General Staff College, 21 April 1995.

Interview at the Navy Connecting Technology Conference with Daniel Kuehl, Chairman of the Information Operations Department, School of Information Warfare and Strategy, National Defense University, Federal Computer Week, Dec 98, 1.

Kennedy, Kevin, Bruce Lawlor, and Arne Nelson. Grand Strategy For Information Age National Security. Policy Analysis Paper. Cambridge: Harvard University, John F. Kennedy School of Government, National Security Program, 22 Aug 1996.

Klinefelter, Stephen. National Security Strategy and Information Warfare. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 23 July 1997.

Libicki, Martin. What Is Information Warfare ?, Fort McNair: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, August 1995.

Metz, Stephen, PhD. Draft Paper - Military Strategy and information Technology: Alternative Visions of Future War. Carlisle Barracks: Strategic Studies Institute, U.S. Army War College, 1999.

Moravec, Hans. Robot: Mere Machine to Transcendent Mind. New York: Oxford University Press, 1999.

Odeen, Philip. Transforming Defense, National Security in the 21st Century. Arlington: National Defense Panel, December 1997.

Orr, Joseph. Information Dominance: A Policy of Selective Engagement. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 24 July 97.

Paret, Peter. Makers of Modern Strategy-From Machiavelli to the Nuclear Age. Princeton, Princeton University Press, 1986.

Pearson, Ian. eds. Atlas of the Future, New York: MacMillan, 1998.

Rochlin, Gener. Trapped in the Net: The Unanticipated Consequences of Computerization. Princeton, Princeton University Press, 1998.

Ross, Michael. National Information Systems: The Achilles Heal of National Security. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 24 July 97.

Russett, Bruce. The Prisoners of Insecurity: Nuclear Deterrence, The Arms Race, and Arms Control. San Francisco, Freeman, 1983.

Sapolsky, Harvey, Eugene Gholz, and Allen Kaufman. "Security Lessons from the Cold War." Foreign Affairs, July/August 1999, 100-113 .

Schement, Jorge, and Terry Curtis. Tendencies and Tensions of the Information Age. New Brunswick: Transaction, 1995.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1995.

Sherman, Jason. "INFOWAR: What Kind of Defense." Armed Forces Journal, August 1997, 36-45.

Slouka, Mark. War of the Worlds: Cyberspace and the High-Tech Assault on Reality, New York: Harper Collins, 1995.

Stewart, Michael. Information Operations, Information Warfare: Policy Perspectives and Implications for the Force. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 24 July 1997.

Sun Tzu. The Art of War, trans. and ed. Samuel Griffith. New York: Oxford University Press, 1982,

Toffler, Alvin, and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. New York: Little, Brown, 1993.

U.S. Congress, Senate, Select Committee on Intelligence, Global Threats and Challenges: The Decades Ahead, Statement of LTG Patrick Hughes, 28 January 1998.

U.S. Department of the Army. Information Operations. Army Field Manual 100-6. Washington D.C.: U.S. Department of the Army, 30 August 1996.

U.S. Department of the Navy. United States Marine Corps. Warfighting, MCDP 1. (Washington D.C.: U.S. Department of the Navy, Headquarters United States Marine Corps, 20 June 1997.

U.S. Joint Chiefs of Staff. Concept for Future Joint Operations: Expanding JV 2010, Washington D.C.: The Joint Staff, May 97.

____. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington D.C.: The Joint Staff, 9 October 1998.

____. Joint Information Operations Policy. CJCSI 3210.01A. Washington D.C.: The Joint Staff, 6 November 1998.

____. Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance, The Joint Staff, 4 July 1995.

Vistica, Gregory. "We're in the Middle of a Cyberwar," NEWSWEEK, 20 September 1999, 88-93.

Whisenhunt, Robert. Information Warfare and the Lack of a U.S. National Policy, Strategy Research Project. Carlisle Barracks: U.S. Army War College, 18 July 1996.